## 1.11 REFERENCES


[1] Zurawski R., "Guest editorial of special section on factory communication systems," IEEE Trans. Ind. Electron., vol. 49, no. 6, pp. 1186-1188, Dec. 2002.

[2] Anastasia G. and Lenzini L., "QoS provided by the IEEE 802.11 wireless LAN to advanced data applications: a simulation analysis", Wireless Networks, vol. 6, no. 99, pp. 99-108, April 2000.

[3] Ferro E. and Potorti F., "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," IEEE Wireless Commun., vol. 12, no. 1, pp. 12-16, Feb. 2005.

[4] Baker, N. "ZigBee and Bluetooth: Strengths and weaknesses for industrial applications," IEE Computing & Control Engineering, vol. 16, no. 2, pp 20-25, April/May 2005.

[5] Lee J. S. and Huang Y. C., "ITRI ZBnode: A ZigBee/IEEE 802.15.4 platform for wireless sensor networks," in Proc. IEEE Int. Conf. Systems, Man & Cybernetics, Taipei, Taiwan, pp. 1462-1467, Oct. 2006.

[6] ZigBee Alliance, Zigbee specification,Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, June 2005.

[7] Mc Innis, M. editor-in-chief, 802.15.4 – IEEE Standard forInformation Technology, Institute of Electrical and Electronic Engineers, New York, 1 October 2003.

[8] Jiang, Y., Cao, J., & Du, Y. (2006). Unmanned air vehicle landing based on Zigbee and vision guidance. *WCICA Vol.* 2, pp 10310 – 10314, May 2006.

[9] Park S.H., Ganz A., Ganz Z. (1998), "Security protocol for IEEE 802.11 wireless local area network", Mobile Networks and Applications,Vol. 3, pp 237–246, May 1998.

[10] Sun K., Ning P., IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006

[11] Zhao T., Nehorai A., "Distributed Sequential Bayesian Estimation of a Diffusive Source in Wireless Sensor Networks", IEEE Transactions on Signal Processing, Vol. 55, No. 4, April 2007

[12] Arifler D., "Information Theoretic Approach to Detecting Systematic Node Destructions in Wireless Sensor Networks", IEEE Transactions On Wireless Communications, Vol. 7, No. 11, November 2008.

[13] Xiaofeng H., Xiang C., "Fault-Tolerant Relay Node Placement in Heterogeneous Wireless Sensor Networks", IEEE Transactions On Mobile Computing, Vol. 9, No. 5, May 2010

[14] Bicakci K., Tavli B., "Prolonging network lifetime with multi-domain cooperation strategies in wireless sensor networks", journal homepage: www.elsevier.com/locate/adhoc, Ad Hoc Networks Vol. 8, pp 582–596, June 2010.

[15] Lung C.H., Zhou C., "Using hierarchical agglomerative clustering in wireless sensor networks": An energy-efficient and flexible approach, journal homepage: www.elsevier.com/locate/adhoc, Ad Hoc Networks Vol. 8, pp 328–344, Feb 2010.

[16] Crescenzo G. D., Ge R., Arce G.R., "Securing Reliable Server Pooling in MANET Against Byzantine Adversaries", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006

[17] Pellegrini F. D., Miorandi D., Vitturi Stefano, and Zanella Andrea "On the Use of Wireless Networks at Low Level of Factory Automation Systems", IEEE Transactions On Industrial Informatics, Vol. 2, No. 2, May 2006.

[18] Lou W., Kwon Y., "A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", IEEE Transactions On Vehicular Technology, Vol. 55, No. 4, July 2006

[19] Doomun M.R. and Soyjaudah KMS, "Analytical Comparison of Cryptographic 8Techniques for Resource-Constrained Wireless Security", International Journal of Network Security, Vol.9, No.1, PP.82–94, July 2009

[20] Zeng P., Cao Z., Choo K.K.R., and Wang S., “Security Weakness in a Dynamic Program Update Protocol for Wireless Sensor Networks”, IEEE Communications Letters, Vol. 13, No. 6, June 2009.

[21] Kosta Y.P, Dalal U.D, Jha Rakesh Kumar, “Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)”, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing.

[22] Poturalski M., Flury M., Papadimitratos P., Hubaux J.P., and Boudec J.Y.L, “Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures”, IEEE Transactions On Wireless Communications, Vol. 10, No. 4, April 2011

[23] Wan Z., Ren K., Zhu B., Preneel B., and Gu M., “Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks”, IEEE Transactions On Vehicular Technology, Vol. 59, No. 2, February 2010

[24] Chao C.M., Lee Y.W., “A Quorum-Based Energy-Saving MAC Protocol Design for Wireless Sensor Networks”, IEEE Transactions On Vehicular Technology, Vol. 59, No. 2, February 2010

[25] Gabrielli A., Mancini L.V., Setia S., and Jajodia S., “Securing Topology Maintenance Protocols for Sensor Networks, IEEE Transactions On Dependable And Secure Computing”, Vol. 8, No. 3, May/June 2011

[26] Gu W., Chellappan S., Bai X., and Wang H. , “Scaling Laws of Key Predistribution Protocols in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security”, Vol. 6, No. 4, December 2011

[27] Zeng P., Choo K.K.R, and Sun D.Z., “On the Security of an Enhanced Novel Access Control Protocol for Wireless Sensor Networks”, IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010

[28] Doomun R., Soyjaudah, “Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security, International Journal of Network Security”, Vol.9, No.1, PP.82–94, July 2009

[29] Amirpoor R., Kumar A., Deavne S.R, “Wirelss Security on Security Standard Policy”: A Case Studty, Reza Amirpoor et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 04, pp 1067-1071, Feb 2010.